IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

KAJEET, INC., Plaintiff, v. MCAFEE CORP., Defendant.	C.A. No. 1:21-cv-00005-MN **JURY TRIAL DEMANDED**

DEFENDANT MCAFEE CORP.'S BRIEF IN SUPPORT OF MOTION FOR SANCTIONS UNDER RULE 11

Susan E. Morrison (#4690)
FISH & RICHARDSON P.C.
222 Delaware Avenue, 17th Floor
P.O. Box 1114
Wilmington, DE 19899
Tel: (302) 652-5070
morrison@fr.com

Aamir A. Kazi
Christopher O. Green
Fish & Richardson P.C.
1180 Peachtree Street NE, 21st Floor
Atlanta, GA 30309
Tel: 404-724-2811
kazi@fr.com
cgreen@fr.com

Attorneys for Defendant McAfee Corp.

Dated: August 23, 2021

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTRODUCTION

Kajeet Inc. ("Kajeet") launched a frivolous lawsuit against McAfee Corp. ("McAfee"), and did so after failing to conduct a reasonable inquiry into the operation of McAfee's accused "Safe Family" product before filing its original or amended complaints. McAfee's Safe Family Product cannot meet a key limitation of every asserted claim—namely the requirement of a server that supervises the activity of a remote device (*e.g.*, a child's mobile phone or tablet computer) by granting or denying requests from the remote device in accordance with a "policy" that is stored on the server itself (and not on the remote device). (*See, e.g.*, D.I. 14, Ex. A at claim 1 ("send to a server a request to communicate with a remote computing device;" "receive in real-time from the server a response . . . based on one or more policies that are stored at the server;" "without accessing the one or more policies by the computing device.").) Had Kajeet conducted any reasonable pre-filing inquiry, as it is obligated to do, it would have recognized this failing.

Put simply, McAfee's Safe Family product does not require server access to enforce its protections, and it therefore cannot meet the claims. McAfee has taken substantial steps since being sued to demonstrate to Kajeet that the Safe Family product cannot infringe any claim of Kajeet's sole asserted U.S. Patent No. 8,667,559 ("the '559 patent")—steps which Kajeet has largely ignored. But McAfee's actions demonstrate that, had Kajeet done a reasonable investigation, it could have come to the conclusion that its allegations were without merit ***before*** filing suit. Specifically, McAfee created a demonstration of its publicly available product, showing that network access is not required for its protections to work—in contravention of the requirements of Kajeet's claims, which require communication between a remote computing device and a server. McAfee also explained how Kajeet could use publicly available tools to observe the timing and type of communications between any device running Safe Family and any server, to confirm the claim requirements are not met. Finally, McAfee made its source code available to Kajeet, so Kajeet could corroborate the other information provided by McAfee.

McAfee has twice asked Kajeet to acknowledge the facially obvious defects in its claims and drop this suit. Kajeet refused in both instances, instead insisting on maintaining this suit in clear derogation of Fed. R. Civ. P. 11. Accordingly, McAfee respectfully requests that the Court dismiss Kajeet's claims and grant this motion for sanctions.

I. NATURE AND STAGE OF PROCEEDINGS

Kajeet initiated this suit on January 4, 2021. (D.I. 1.) Soon after, McAfee moved to dismiss Kajeet's claims of direct infringement, indirect infringement, willful infringement, and past damages. (D.I. 10.) As to Kajeet's infringement theory, McAfee pointed out that Kajeet's infringement allegations, even if accepted as pleaded, failed to show how the Safe Family application communicated decision-making with a remote server in "real-time." (*Id.* at 11-12.) Effectively conceding that its original complaint was deficient, Kajeet responded by filing an amended complaint on April 12, 2021. (D.I. 14.) But the amended complaint does not correct the deficiencies McAfee identified in the original complaint—including the requirement of "real-time" communication set forth in McAfee's motion without accessing locally stored policies. Thus, McAfee filed a Motion to Dismiss Kajeet's First Amended Complaint. (D.I. 18.)

McAfee's Motion to Dismiss Kajeet's First Amended Complaint remains pending.

II. SUMMARY OF ARGUMENT

1. Kajeet had full ability and access to observe and test the allegedly infringing operations of McAfee's accused Safe Family product before filing this lawsuit, but failed to do so. If Kajeet had tested the accused Safe Family product and compared the results to the

elements of the ’559 patent claims, the distinctions between the accused product and the asserted claims would have been facially obvious. Kajeet thus failed to conduct a pre-suit “reasonable inquiry” as required by Rule 11 and should be sanctioned.

2. Similarly, Kajeet insists on continuing this suit despite McAfee demonstrating why the Safe Family product cannot infringe the ’559 patent claims. McAfee has even offered its product source code to Kajeet for an inspection, which would corroborate the facially obvious defects in Kajeet’s infringement allegations. Rule 11 likewise prohibits a plaintiff from maintaining a cause of action once it becomes apparent that the plaintiff’s factual contentions lack evidentiary support.

3. Kajeet’s failure to follow the basic requirements of Rule 11 has caused both McAfee and the Court to spend significant resources addressing a meritless suit. The Court should dismiss Kajeet’s claims with prejudice and award McAfee its attorney fees.

III. STATEMENT OF FACTS

A. Kajeet’s ’559 Patent and Asserted Claims 1 and 27 Require A Remote Server to Make Real-Time “Grant” or “Deny” Decisions

The ’559 patent issued on March 4, 2014, and is titled “Feature Management of a Communication Device.” (D.I. 14, Ex. A.) According to the ’559 patent, parents, school administrators, and employers may want the ability to control and/or restrict how and when children, students, and employees use cellphones or other electronic devices. (*Id.* at 1:66-2:26.)

The system disclosed in the ’559 patent purports to solve this problem by providing, in a cellular telephone network, a “policy enforcement point (PEP) 28” containing policies that determine whether a particular device may be used for particular purposes. (*Id.* at 8:36-40.) The PEP works in conjunction with a “policy decision point (PDP) 29,” which “maintains or stores a list of policies that have been established to control the features and functions of the mobile [device] and decides, based on those policies, to either accept or reject" any attempt by the phone to request service from the network. (*Id.* at 8:40-59.) As can be seen in Figure 2, both the PEP and PDP are parts of the telephone network, and neither resides on the mobile station 10 (*i.e.*, the mobile phone or other user device). (*Id.* at Fig. 2.)

It is this remote enforcement of a remotely stored policy, by accepting or rejecting attempts by the mobile device to communicate over the network, that provides the supposed advantage of the invention: a tamper-proof ability to control network access by a device. Kajeet repeatedly emphasizes this point in its amended complaint when describing the alleged benefits of the claimed invention and how it differed from the prior art:

- "Application of use decisions based upon ***a policy stored remote from the controlled computing device*** represented an unconventional scheme that was neither well known nor routine for addressing a newly emerging problem in society." (*Id.* at ¶ 19.)

- "These claimed methods require, among other steps, that a decision is received in real-time from a server, with the decision 'being ***based on a policy stored at the server . . .*** ,' and that 'the communication being enabled or disabled ***without storing the policy on the computing device***.'" (*Id.* at ¶ 36.)

- "These limitations mandate that the decision applied to effect control over the computing device is ***based on a policy stored at a server remote to the computing device . . . .*** These limitations capture the distributed architecture concept not well-understood, routine, or conventional in the art for effecting feature management on a computer device including that ***the server storing the policies upon which decisions are based being meaningfully apart from the computing device***. This arrangement resulted in improved operation through at least increase resilience to undesirable access to policies to manipulate or delete them." (*Id.* at ¶ 37 (emphasis of "not" in original).)

- "These claims require storing usage policies upon which decisions are based ***at a server remote from the computing device***, an unconventional arrangement at the time which yielded improvements in the operation of systems implementing the claimed methods. Prior art control was not premised on application of decisions based upon policies stored at the server level. Instead, ***the prior art applied decisions based on policies set up on the computing device itself*** and stored only on the computing device. Such policies reside such that they are readily accessible for manipulation and/or deactivation or deletion to circumvent control entirely." (*Id.* at ¶ 40.)

The role of the server in granting or denying requests ***in real-time*** to communicate with a remote device based on a policy ***stored at the server*** is also recited by the asserted claims:

> 1. A non-transitory computer readable storage medium comprising instructions that, when executed on a computing device configured to perform a function on a communication network managed by a service provider, cause the computing device to at least:
>
> > ***send to a server*** a request to communicate with a ***remote*** computing device over the communication network;
> >
> > ***receive in real-time*** from the server a response indicative of a decision granting or denying the request, the decision being based on one or more ***policies that are stored at the server*** and based at least in part on input from an administrator; and
> >
> > enforce the response by enabling the requested communication with the ***remote*** computing device over the communication network when the decision grants the request and by disabling the requested communication when the response denies the request, the requested communication being enabled or disabled ***without accessing the one or more policies*** by the computing device.
>
> * * *
>
> 27. A method for controlling a computing device configured to execute a function using a communication network managed by a service provider, the method comprising:
>
> > ***sending to a server*** a request to communicate with a ***remote*** computing device over the communication network;
> >
> > receiving ***in real-time*** from the server a decision granting or denying the request, the decision being ***based on a policy stored at the server*** and configured by an administrator; and
> >
> > enforcing the decision by enabling a communication with the ***remote*** computing device over the communication network when the decision grants the request and by disabling the communication when the decision denies the request, the communication being enabled or disabled ***without storing the policy on the computing device***.

(D.I. 14, Ex. A at claims 1, 27). Thus, the limitations relevant to this motion require that (i) the server applies the policy to provide, "in real-time," a "decision[s] granting or denying" such requests, and (ii) that the policy that determines whether to grant or deny a request is not "stor[ed]" on (in claim 27) or "access[ed]" at (in claim 1) the computing device itself.

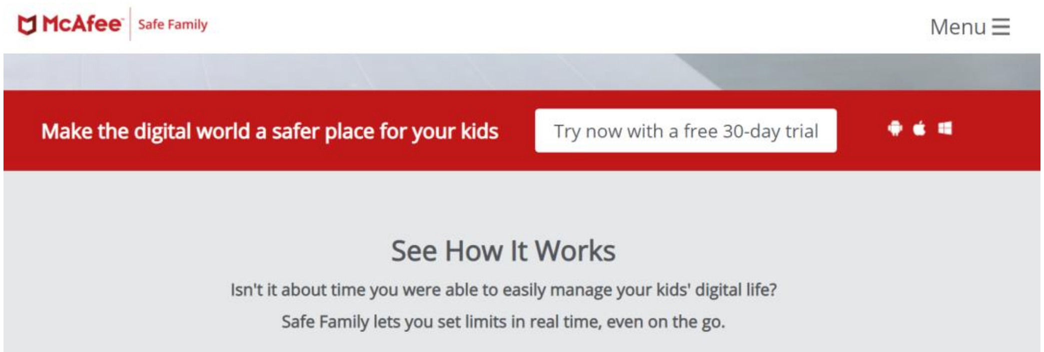
This requirement is confirmed by the court's claim construction order in *Kajeet, Inc. v. Qustodio, LLC*, No. SA CV18-01519 (C.D. Cal. Nov. 1, 2019) at 13 (attached hereto as Exhibit A). In concluding that claim 27 of the '559 patent should be given its ordinary meaning, the court observed that "[t]he requirement that ***both storing a policy and enforcing a decision occur remotely*** is apparent from the express claim language . . . . Because the parties cannot reasonably dispute that the plain claim language that shows that the claimed policy and claimed enforcement step in Claim 27 of the '559 Patent occur remote from the computing device, no further construction of these claim terms is necessary." *Id.*

Notably, McAfee set forth these exact same statements regarding the '559 patent and the scope of its claims in its pending motion to dismiss Kajeet's first amended complaint, including specifically the facially apparent claim limitations requiring a remote server to make grant/deny decisions, in real-time, based on a "policy" that is not stored on the device under control. (D.I. 18 at 4–6.) Were any aspect of McAfee's interpretation of the claims inaccurate (or even debatable), Kajeet presumably would have made its contrary interpretation of the '559 patent claims known in its opposition (D.I. 21). Kajeet, however, said nothing.

B. McAfee's Safe Family Product Does Not Receive Real-Time "Grant" or "Deny" Decisions From A Remote Server

McAfee's Safe Family product does not perform the unambiguous claim requirements accessing "policy" information stored on a "remote server" in real-time for purposes of "grant" or "deny" decisions. Instead, McAfee's Safe Family product stores all rules locally on the protected device (*i.e.*, a smartphone) and relies on that device for decision-making—not some "remote server." Kajeet could and should have discovered this basic fact via a pre-suit investigation.

McAfee's Safe Family product is a publicly available application available for download for a free trial period at https://family.mcafee.com/ as shown in the screen capture below:



McAfee | Safe Family

Make the digital world a safer place for your kids

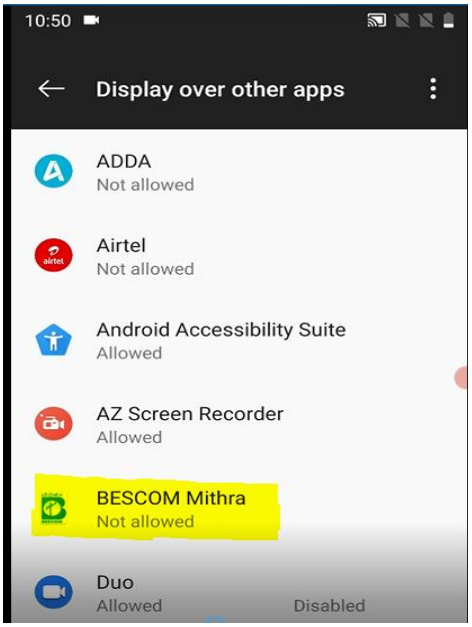
See How It Works

Isn't it about time you were able to easily manage your kids' digital life?

Safe Family lets you set limits in real time, even on the go.

Using this free download, Kajeet could have quite easily determined that rules set in the application—such as the screen time restriction referenced in Kajeet's amended complaint (D.I. 14 at ¶ 29)—are stored and/or accessed locally and ***not*** resident on a remote server.

For example, the screen captures below show an example of what Kajeet would have seen if it had performed the requisite pre-filing analysis:



Display over other apps

ADDA
Not allowed

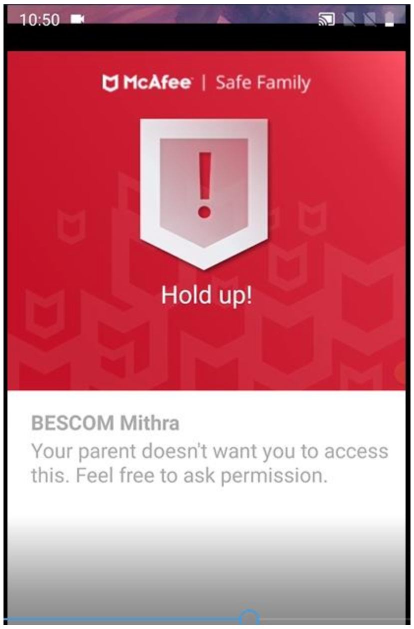
Airtel
Not allowed

Android Accessibility Suite
Allowed

AZ Screen Recorder
Allowed

BESCOM Mithra
Not allowed

Duo
Allowed Disabled



McAfee | Safe Family

Hold up!

BESCOM Mithra

Your parent doesn't want you to access this. Feel free to ask permission.

These screen captures were taken from a demonstration of a mobile phone running the Safe Family application while completely disconnected from data networks (*i.e.*, no cellular data service and no Wi-Fi). Thus, any information utilized during the demonstration could not have been dependent upon a "remote server."

In the example above, the mobile device contains an application for BESCOM Mithra (distributed by a telecom service provider in India, where this test was conducted at one of McAfee's international development facilities) that the user of the phone is not allowed to access (*see* above left graphic). The screen shot further shows other applications that the user is allowed to access (such as Android Accessibility Suite, AZ Screen Recorder, and Duo). The device sets forth the rules for the listed applications without accessing a "remote server" in real-time (again, because the absence of network connectivity precluded the mobile device from making ***any*** communications). When the user attempts to access an application that is "Allowed," Safe Family permits it. But if the user attempts to access an application that is "Not allowed" (such as the BESCOM Mithra application), Safe Family blocks the attempt and displays a message (shown above at right) alerting the user that separate permission must be requested from the policy administrator (e.g., a parent).

Importantly, Kajeet would be able to observe from testing that a mobile device running McAfee's Safe Family application solely relies on locally stored information, and that fact removes any possibility of infringing the '559 patent claims. The Safe Family application is not designed to function one way when a network is present (e.g., by accessing remotely stored "policies" governing user activity), but in another way when network connectivity is removed (by accessing locally stored "policies" as shown above). Thus, a straightforward test of the Safe Family application would show that regardless of whether the device is network-connected, the application functions in a manner distinct from the asserted ’559 claims. And this form of operational test is but one way Kajeet could (and should) have verified whether Safe Family makes real-time inquiries of a remote server to enforce policy decisions.

C. McAfee Notified Kajeet of its Flawed Theory

Shortly after Kajeet filed its First Amended Complaint, McAfee sent Kajeet a letter that informed Kajeet that “Safe Family does not rely on retrieving, in real-time, ‘policy’ information from a server.” (Ex. A, A. Kazi Letter to C. Vowell of April 26, 2021.) McAfee noted that “Kajeet could verify quite easily that restrictions set in the application (such as the screen time restriction referenced in Kajeet’s amended complaint) are enforced even when the device has disabled all network settings.” *Id.*

After Kajeet refused to dismiss its case, McAfee provided Kajeet with a demonstration of the product substantiating McAfee’s statements. (Ex. B, A. Kazi Letter to C. Vowell of June 17, 2021.) McAfee also identified other tests (such as using a tool to monitor communications over the network) that Kajeet could perform if it found the information McAfee provided unavailing for some reason:

> The operation of McAfee’s Safe Family product, including the demonstration we referenced above, indisputably shows that Safe Family maintains policy information locally. Kajeet has no good faith basis for stating that a device running the Safe Family application operates differently when connected to a network, and even this point is once again something that Kajeet could have, and should have, investigated to satisfy its Rule 11 obligations. For example, Kajeet could use a packet sniffing tool (such as WireShark) to observe the timing and type of communications between any device running Safe Family and any server. From those communications, it is also clear that policy information is not accessed in real time at the server. Thus, as we have indicated to you on prior occasions, the Safe Family application, when running on a device, does not perform the recited requirements of communicating with a remote server in “real time” to have requests granted or denied based on policies that “are stored at the server” and that are not accessed by the device itself.

(Ex. B, A. Kazi Letter to C. Vowell of June 17, 2021.)

To remove any doubt, McAfee has made its source code available for inspection. Thus, McAfee provided Kajeet with evidence of how Safe Family operated, described the steps that Kajeet could take to replicate this testing, identified publicly available tools (WireShark) Kajeet could use to test additional scenarios, and made its source code available for Kajeet to inspect.

Lastly, in advance of filing this motion, McAfee provided Kajeet with a copy of this motion and requested one final time that Kajeet withdraw its claims. Kajeet never responded.

IV. LEGAL STANDARDS

Rule 11 of the Federal Rules of Civil Procedure allows a court to impose sanctions for frivolous legal arguments or baseless factual assertions. Fed. R. Civ. P. 11(b)(2)-(3). To satisfy Rule 11's pre-filing requirement in a patent infringement lawsuit, the patentee's attorney must, "at a bare minimum, apply the claims of each and every patent that is being brought into the lawsuit to the accused device and conclude that there is a reasonable basis for a finding of infringement of at least one claim of each patent so asserted." *View Eng'g. Inc. v. Robotic Vision Sys., Inc.*, 208 F.3d 981, 986 (Fed. Cir. 2000) ("The presence of an infringement analysis plays the key role in determining the reasonableness of the pre-filing inquiry made in a patent infringement case under Rule 11.") (emphasis added); *S. Bravo Sys., Inc. v. Containment Techs. Corp.*, 96 F.3d 1372, 1375 (Fed. Cir. 1996). This pre-filing investigation is particularly important in patent cases because "[a] patent suit can be an expensive proposition. Defending against baseless claims of infringement subjects the alleged infringer to undue costs." *View Eng'g. Inc.*, 208 F.3d at 986.

V. ARGUMENT

This case is a textbook example of frivolous patent litigation. The claims unequivocally require that when a local device seeks to perform a function, the local device receives a decision in real-time from a remote server indicating whether it can perform that function or not. ('559 Pat. at claim 1 ("receive in real-time from the server a response indicative of a decision granting or denying the request . . ."); *id.* at claim 27 ("receiving in real-time from the server a decision granting or denying the request").) And the claims further require that the device does not access the policy information locally. (*Id.* at claim 1 ("the requested communication being enabled or disabled without accessing the one or more policies by the computing device"); claim 27 ("the communication being enabled or disabled without storing the policy on the computing device").) Yet, any reasonable diligence would show that McAfee's Safe Family does not satisfy these limitations.

Kajeet points to nothing to substantiate its infringement theory. Kajeet's Complaint and Amended Complaint lacks any such showing. (*See*, *e.g.*, D.I. 10 (McAfee's Motion to Dismiss Complaint); D.I. 18 (McAfee's Motion to Dismiss Amended Complaint).) The Amended Complaint includes generic allegations, but no facts showing "real-time" communications. (*See*, *e.g.*, D.I. 23 at 1-2.) Because of this, McAfee moved to dismiss Kajeet's Amended Complaint and while that motion is pending, has repeatedly asked Kajeet to provide its basis for maintaining suit:

> To the extent that Kajeet continues to allege (as the asserted claims plainly require) that Safe Family receives real-time responses from a server indicative of a decision granting or denying a request—based on "policies" stored at the server and not accessed by the device itself (as the asserted claims clearly require)—please provide that basis now. Notably, Kajeet's prior letter makes vague reference to "extensive publicly available documentation," but Kajeet has yet to identify a single specific document as a basis for satisfying its Rule 11 obligations.

(Ex. B, A. Kazi Letter to C. Vowell of June 17, 2021.) Although Kajeet refers to "extensive" documentation it has reviewed, thus far ***it has yet to identify a single document or piece of evidence*** supporting its allegations. (Ex. C, C. Vowell Letter to A. Kazi of May 14, 2021 (referring to the "extensive publicly available documentation" that Kajeet had purportedly relied upon); Ex. D, C. Vowell Letter to A. Kazi of July 2, 2021 (referring to the "publicly available materials" that Kajeet purports to rely upon).)

Kajeet's recently served infringement contentions confirm this gap in Kajeet's infringement theory. Kajeet's infringement contentions show only that Safe Family allows parents to limit the usage of their child's devices by setting policies, and that those policies can be set through a networked device. Kajeet makes no showing of "real-time" decision making at the remote server. Kajeet also fails to substantiate its theory that policy information is not stored or accessed locally.

Any reasonable investigation would have revealed the opposite is true—that McAfee's Safe Family ***does*** store information locally. For example, as shown in the demonstration of the Safe Family product, McAfee's Safe Family product includes rules for various applications. Those rules are visible to the user through the graphical menu and they are enforced regardless of whether the Safe Family application is connected to the network or not. Kajeet could have and should have tested this functionality in Safe Family before filing suit. Kajeet alleges that McAfee's testing is inconclusive, but McAfee then encouraged Kajeet to perform its own tests and even identified the publicly available network communications tool (WireShark) that Kajeet could have used. But Kajeet has done nothing, and has made no effort to investigate McAfee's source code, which McAfee made available for Kajeet to confirm the operation of Safe Family.

Kajeet's infringement allegations lacked any factual support from the time the Complaint was filed. McAfee undertook to do Kajeet's work for it, creating a product demonstration proving beyond doubt that the complaint is laden with meritless infringement allegations. (Ex. B, A. Kazi Letter to C. Vowell of June 17, 2021.) Yet Kajeet persists, and hides its head in the sand to avoid the evidence McAfee has presented. And while it ignores McAfee's evidence, Kajeet has not offered a single bit of evidence to refute the facts McAfee has presented. Kajeet choice to abdicate all its responsibilities under the Federal Rules, and to ignore all facts that show its case to be meritless, must have consequences.

Kajeet's failure to meet its obligations under Rule 11 has caused McAfee substantial harm and merits an award of sanctions. Kajeet has forced McAfee to expend considerable time, effort, and resources to defend itself against Kajeet's baseless claims—claims that Kajeet should have known were baseless upon a reasonable inspection of the publicly available information about McAfee's Safe Family product. Moreover, unless Kajeet's meritless infringement claims are dismissed with prejudice, McAfee will continue to be harmed by Kajeet's failure to abide by the basic tenants of the Federal Rules of Civil Procedure and established case law.

Thus, under the authority granted by Rule 11, this Court should dismiss Kajeet's infringement claims with prejudice and award McAfee its attorneys' fees and costs for defending against those claims.

VI. CONCLUSION

Kajeet's failure to comply with Rule 11's pre-filing investigation requirement mandates an award of sanctions. Accordingly, McAfee respectfully requests that the Court dismiss Kajeet's claims under the '559 patent with prejudice and award McAfee all of its fees and costs incurred in defending this suit.

Dated: August 23, 2021

By: */s/ Susan E. Morrison*
Susan E. Morrison (#4690)
FISH & RICHARDSON P.C.
222 Delaware Avenue, 17th Floor
P.O. Box 1114
Wilmington, DE 19899
Tel: (302) 652-5070
morrison@fr.com

Aamir Kazi
Christopher O. Green
Fish & Richardson P.C.
1180 Peachtree Street NE, 21st Floor
Atlanta, GA 30309
Tel: 404-724-2811
kazi@fr.com
cgreen@fr.com

ATTORNEYS FOR DEFENDANT
MCAFEE CORP.